TAGPMA

The Americas Grid
Policy Management Authority

TAGPMA Update

Derek Simmel dsimmel@psc.edu, TAGPMA Chair

48th EUGridPMA Meeting

CESNET, Metacentrum

Prague, Czech Republic

January 22, 2020

TAGPMA Leadership

- Chairs: Derek Simmel dsimmel@psc.edu (PSC, U.S.A.)
  Paula Venosa pvenosa@info.unlp.edu.ar (UNLP, Argentina)
- Vice-chair: Ale Stolk alestolk@gmail.com (ULAGrid, Venezuela)
- Secretary: Jeny Teheran, jteheran@fnal.gov (Fermilab, U.S.A.)
- Web Master: Scott Sakai ssakai@sdsc.edu (SDSC, U.S.A.)

TAGPMA Members

Organization	Country	Representative	Member Type
FNAL	U.S.A.	Jeny Teheran	Relying Party
OGF	U.S.A.	Alan Sill	Relying Party
OSG	U.S.A.	Susan Sons	**Relying Party**
REBCA	U.S.A.	Scott Rea	Relying Party
SDSC	U.S.A.	Scott Sakai	Relying Party
UFF	Brazil	Vinod Rebello	Relying Party
ULAGrid	Venezuela	Ale Stolk	Relying Party
UNIANDES	Colombia	Andres Holguin	Relying Party
WLCG	Switzerland	David Kelsey	Relying Party
XSEDE	U.S.A.	**Derek Simmel**	Relying Party
DigiCert	U.S.A.	Tomofumi Okubo	Authentication Provider
GridCanada	Canada	Lixin Liu	Authentication Provider
IBDS ANSP	Brazil	Angelo de Souza Santos	Authentication Provider
InCommon	U.S.A.	Jim Basney	Authentication Provider
NCSA	U.S.A.	Jim Basney	Authentication Provider
NERSC	U.S.A.	Jeff Porter	Authentication Provider
PSC	U.S.A.	Derek Simmel	Authentication Provider
REUNA	Chile	Alejandro Lara	Authentication Provider
UNAM	Mexico	Jhonatan Lopez	Authentication Provider
UNLP	Argentina	Paula Venosa	Authentication Provider

TAGPMA Members

- 20 Members (10 APs, 10 RPs) from the North, Central and South American countries + Switzerland
  - Including Argentina, Brazil, Canada, Chile, Colombia, Mexico, U.S.A and Venezuela, + WLCG (RP) in Switzerland

- 19 IGTF-Accredited CAs (as of distribution v.1.102, October 2019)
  - 13 Classic CAs
    - Argentina: UNLPGrid
    - Brazil: ANSPGrid
    - Canada: GridCanada
    - Chile: REUNA
    - Mexico: UNAM (2)
    - U.S.A.: DigiCert(6), InCommon (IGTF Server CA)
  - 4 Short Lived Credential Service (SLCS) CAs
    - U.S.A.: NCSA (SLCS-2013, TFCA-2013), PSC
    - **NERSC plans to retire their SLCS CA**
  - 1 Member-Integrated Credential Service (MICS) CA
    - U.S.A.: NCSA (CILogon-Silver)
  - 1 Identifier-Only Trust Assurance (IOTA) CA
    - U.S.A.: NCSA (CILogon-Basic)

TAGPMA Communications

- TAGPMA Website: http://www.tagpma.org
  - Public information and documents
  - Now hosted on Google Sites
    - **Needs to be migrated to new-style Google Sites, or to another usable platform…**
    - Focus of TAGPMA Officers' Meeting March 2020
- Mailing lists:
  - tagpma-general – subscribe by joining the tagpma-general Google Group
  - tagpma-private – members-only mailing list currently maintained at PSC
- TAGPMA Slack Channel
  - Join group **tagpma.slack.com**
- E-mail any suggestions or issues directly to the Chair (dsimmel@psc.edu)

TAGPMA Conference Calls

- Monthly conference calls:
  - Currently scheduled on the 2nd Tuesday of every Month*
  - Spanish language call TBD*
  - English language call begins at 1:00pm (U.S. Eastern, currently UTC -5:00)*
  - Zoom link
    - https://cmu.zoom.us/j/598670138
    - Backup: Vidyo link at https://www.nikhef.nl/grid/video/?m=tagpma

  *times and dates change periodically to maximize member availability

- All IGTF members and prospective TAGPMA members are welcome to attend and participate in TAGPMA meetings!
  - Contact the Chair (dsimmel@psc.edu) for current call times and coordinates

TAGPMA Meetings

- 28th TAGPMA F2F Meeting @ Internet2 Technology Exchange
  - December 13, 2019, New Orleans, Louisiana, U.S.A.

- TAGPMA Officers Meeting – Focus on TAGPMA website
  - March 12-13, 2020, San Diego, CA, U.S.A.

- 2020 TAGPMA F2F Meeting Planning – Colocation ideas:
  - August 31-September 2: RedClara/TICAL conference, Ecuador
  - October 5-8: Internet2 Technology Exchange, Atlanta, GA, U.S.A.

- IGTF All-Hands Meeting Planning, Sept-Nov timeframe 2020
  - Proposed: NCSA to host in Champaign–Urbana, Illinois before or after U.S. NSF CyberSecurity Summit (Indianapolis, Indiana, Sept 22-24, 2020)

28th TAGPMA F2F Meeting Highlights

- Agenda and presentation slides at https://indico.rnp.br/event/13/

- Assurance for JWT (JSON Web Tokens) [Jim Basney, NCSA]
  - WLCG Common JWT Profiles
  - Adoption by SciTokens (Fed AuthZ tools project) https://scitokens.org
- GridCanada CA redesign discussion
- Peer Review of REFEDS Assurance Adoption
  - Checklists drafted by Jim Basney
    - REFEDS Assurance Framework, Single Factor Authentication, Multifactor Authentication
  - Reviewed checklists completed for XSEDE IdP and Fermilab IdP

REFEDS Assurance Framework Checklist Template

Assertion	Description	Required for Cappuccino	Required for Espresso	Meets Requirement?
https://refeds.org/assurance	1. The Identity Provider is operated with organizational-level authority.	Yes	Yes	FALSE
	2. The Identity Provider is trusted enough that it is (or it could be) used to access the organization's own systems.			FALSE
	3. Generally-accepted security practices are applied to the Identity Provider.			FALSE
	4. Federation metadata is accurate, complete, and includes at least one of the following: support, technical, admin, or security contacts.			FALSE
https://refeds.org/assurance/ID/unique	(Unique-1) The user identifier represents a single natural person.	Yes	Yes	FALSE
	(Unique-2) The CSP can contact the person to whom the identifier is issued.			FALSE
	(Unique-3) The user identifier is never re-assigned.			FALSE
	(Unique-4) The user identifier is eduPersonUniqueId, SAML 2.0 persistent name identifier, subject-id or pairwise-id or OpenID Connect sub (type: public or pairwise).			FALSE
https://refeds.org/assurance/ID/eppn-unique-no-reassign	eduPersonPrincipalName value has the Unique-1, Unique-2 and Unique-3 properties.			FALSE
https://refeds.org/assurance/ID/eppn-unique-reassign-1y	eduPersonPrincipalName value has the Unique-1 and Unique-2 property but may be re-assigned after a hiatus period of 1 year or longer.			FALSE
https://refeds.org/assurance/IAP/low	Identity proofing and credential issuance, renewal, and replacement qualify to any of: - sections 5.1.2-5.1.2.9 and section 5.1.3 of Kantara assurance level 1 - IGTF level DOGWOOD - IGTF level ASPEN Example: self-asserted identity together with verified e-mail address, following sections sections 5.1.2-5.1.2.9 and section 5.1.3 of [Kantara SAC].	Yes	Yes	FALSE
https://refeds.org/assurance/IAP/medium	Identity proofing and credential issuance, renewal, and replacement qualify to any of: - sections 5.2.2-5.2.2.9, section 5.2.2.12 and section 5.2.3 of Kantara assurance level 2 - IGTF level BIRCH - IGTF level CEDAR - section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low Example: the person has sent a copy of their government issued photo-ID to the CSP and the CSP has had a remote live video conversation with them, as defined by [IGTF].	Yes	Yes	FALSE
https://refeds.org/assurance/IAP/high	Identity proofing and credential issuance, renewal, and replacement qualifies to any of: - section 5.3.2-5.3.2.9, section 5.3.2.12 and 5.3.3 of Kantara assurance level 3 - section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level substantial Example: the person has presented an identity document that is checked to be genuine and represent the claimed identity and steps have been taken to minimise the risk of a lost, stolen, suspended, revoked or expired document, following sections 2.1.2, 2.2.2 and 2.2.4 of eIDAS assurance level substantial [eIDAS LoA].		Yes	FALSE
https://refeds.org/assurance/IAP/local-enterprise	The identity proofing and credential issuance, renewal and replacement are done in a way that qualifies (or would qualify) the user to access the Home Organisation's internal administrative systems (see appendix A).			FALSE
https://refeds.org/assurance/ATP/ePA-1m	eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within 31 days time (*) The CSP can omit this requirement if it doesn't populate and release the eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attribute values.	Yes (if applicable)	Yes (if applicable)	FALSE
https://refeds.org/assurance/ATP/ePA-1d	eduPersonAffiliation, and eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within one days time.			FALSE

REFEDS SFA Checklist Template

Description	Meets Requirement?
4.1 The authentication factor fulfills the following requirements:	
4.1.1 Authenticator secrets have at least the following minimum length: [REFER TO TABLE IN PROFILE]	FALSE
4.1.2 Secrets that are transmitted must have a maximum life span according to the way of delivery. Time based OTP Device: 5 minutes Telephone network (e.g. SMS, phone): 10 minutes E-mail (e.g. recovery link): 24 hours Postal mail: 1 month	FALSE
4.1.3 Accounts are protected against online guessing attacks (e.g. rate limiting).	FALSE
4.1.4 Authentication secrets at rest and in online transit must be cryptographically protected.	FALSE
4.2 Replacement of a lost authentication factor ensures all of the following, as applicable:	
4.2.1 An existing secret must not be sent to the user (e.g. a stored password).	FALSE
4.2.2 The replacement procedure does not solely rely on knowledge-based authentication (e.g. answer a secret question).	FALSE
4.2.3 Human based procedures (e.g. service desk) ensure a comparable level of assurance of the requesting user identity as the initial identity vetting.	FALSE
4.2.4 In order to restore a lost authentication factor, an OTP may be sent to the users address of record. All corresponding requirements apply as though this OTP would be a Look-Up Secret, except that it may be transmitted without being cryptographically protected.	FALSE
4.2.5 For authenticators which are provided to the user as a backup, all requirements of the corresponding authentication factor apply.	FALSE

REFEDS MFA Checklist Template

Description	Meets Requirement?
The authentication of the user's current session used a combination of at least two of the four distinct types of factors defined in ITU-T X.1254: Entity authentication assurance framework, section 3.1.3, authentication factor (something you know, something you have, something you are, something you do)	FALSE
The factors used are independent, in that access to one factor does not by itself grant access to other factors.	FALSE
The combination of the factors mitigates single-factor only risks related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor.	FALSE

- Thanks to Jim Basney for drafting these checklists!
- Complete procedure for IGTF accreditation (?) to be developed…
- Comments, questions, suggestions welcomed

REFEDS Checklist Review Exercise: FNAL

- Assurance Framework:
  - FNAL IdP asserts IAP/low and IAP/medium only.
  - FNAL IdP does not assert ID/eppn-unique-reassign-1y. (Not applicable)
  - eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within 31 days' time
- SFA Profile:
  - 4.2.5 For authenticators which are provided to the user as a backup, all requirements of the corresponding authentication factor apply: FALSE (User contacts help desk to create new password)

REFEDS Checklist Review Exercise: XSEDE

- Assurance Framework
  - XSEDE IdP asserts IAP/low, IAP/medium, and IAP/local-enterprise.
    - XSEDE IdP should stop asserting IAP/local-enterprise as it is not a Home Organization
  - (Unique-1) The user identifier represents a single natural person: FALSE
    - XSEDE asserts this for every user account that is part of an allocated project – for which user vetting is required and users acknowledge compliance with policies against account sharing – but the existence of XSEDE “community accounts” violates this assertion
  - ID/eppn-unique-no-reassign: FALSE
    - Although XSEDE does not reassign identifiers, the unique-1 violation breaks this as well
  - XSEDE IdP does not assert ID/eppn-unique-reassign-1y. (Not applicable)
  - XSEDE IdP does not assert attributes reflecting user departure.
- MFA Profile
  - XSEDE Meets all MFA requirements